DoD Privacy Impact Assessment (PIA)

1. Department of Defense (DoD) Component.

United States Air Force (USAF)

2. Name of Information Technology (IT) System.

Air Force Directory Services (AFDS)

3. Budget System Identification Number (SNAP-IT Initiative Number).

0258

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)).

1737

5. IT Investment (OMB Circular A-11) Unique Identifier (if applicable).

007-57-03-54-01-0258-00

6. Privacy Act System of Records Notice Identifier (if applicable).

A System of Records Notice (SORN) for AFDS, F033 AF E, was published in the Federal Register, February 25, 2005, 70 FR 9283.

7. OMB Information Collection Requirement Number (if applicable) and Expiration Date.

Not Applicable.

8. Type of authority to collect information (statutory or otherwise).

10 United States Code (USC) 8013, Secretary of the Air Force; Air Force Instruction 33-202, Volume 6, Identity Management; and Executive Order (EO) 9397 (SSN – Social Security Number)

9. Provide a brief summary or overview of the IT system (activity/purpose, present lifecycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup).

- Air Force Directory Services (AFDS) architecture facilitates data transparency for Air Force systems and applications by providing Authoritative Data Sources for the purpose of identity management

- Creates central repository for identity data which, through aggregation of data, provides a more complete and accurate record than that of individual data sources

- AFDS infrastructure is composed of integrated components used to effectively manage access control, identity data management, and security threats for the Air Force Enterprise - Key enabler of Public Key Infrastructure (PKI)

- Supports Chief Secretary of the Air Force's (CSAF) goal of Net-Centric warfare through access to consolidated Enterprise Services

- Foundation for single Air Force enterprise authentication service

- Integrated Air Force solution for sharing information

- AFDS consolidates and distributes the Air Force Global Address List (GAL) to all Major Commands (MAJCOMs), Combatant Commands (COCOMs) and supporting agencies – essential to maintaining Warfighter communications

- AFDS is the standard Air Force directory service that ensures the right data get to the right people when needed and restricts access to unauthorized users

- AFDS ensures identity data integrity and security for directory access of all major Air Force programs

10. Describe what information in identifiable form will be collected and the nature and source of the information (e.g. names, Social Security Numbers, gender, race, other component IT systems, IT systems from agencies outside Department of Defense (DoD), etc.).

AFDS does not gather or disseminate any identity data in identifiable form. All data are transmitted via Secure Light Directory Access Protocol (LDAP) or Hyper Text Transport Protocol in a Secure Sockets Layer encrypted session (HTTPS) using approved DoD Encryption methodologies. The only exception to this rule is the identity data stored in the system that the individual can review on himself or herself. AFDS pulls and stores the following type of information: Name, Electronic Data Interchange Personal Identifier (EDIPI), Social Security Number, Social Security Number Type, Date of Birth, Gender, Citizenship Status, Major Command (MAJCOM), Base Name, Office Symbol, Assigned and Attached Unit/PAS (personal accounting symbol), Personnel Category Code, Duty Assigned Code, Generational Qualifier, Pay Plan, Pay Grade, Rank, Reservist/ANG (Air National Guard) Category Code, Non-Publish Status (Protected Airman), Telephone Number, Fax Number, e-Mail Address, DoD PKI Certificate.

11. Describe how the information will be collected (e.g., via the Web, via paper-based collection, etc.).

Records within AFDS are derived from data originating from the following official DoD systems: Military Personnel Data System (MilPDS), Defense Manpower Data Center (DMDC),

Defense Civilian Personnel Data System (DCPDS) (Data Processing Resources - DPR 34), Global Directory Services (GDS), and the Air Force Global Address Listing (AFGAL). Selected authoritative data are pulled from each of these systems via Secure LDAP and HTTPS using DoD approved Encryption methodologies.

12. Describe the requirement and why the information in identifiable form is to be collected (e.g., to discharge a statutory mandate, to execute a Component program, etc.).

AFDS Program Management Office (PMO) was established to address enterprise Information Technology challenges and to enhance mission performance through seamless integration of information providing data transparency to Air Force and DoD applications requiring identity data in the accomplishment of their mission and reducing overall costs associated with stovepipe connections. AFDS is the key enabler for a single Air Force Authentication services and Chief Staff of the Air Force's (CSAF) goal of Net-Centric warfare through access to consolidated Enterprise Services. The collection and use of the data are both relevant and necessary to the purpose for which the system is designed.

Air Force Directory Services does not collect or disseminate information in identifiable form. All information is transmitted via Secure LDAP and HTTPS using DoD approved encryption methodologies.

13. Describe how the information in identifiable form will be used (e.g., to verify existing data, etc.).

AFDS provides the Air Force a meta-directory that is an aggregate of existing data to provide a single data source of Air Force member's identity information for DoD applications. In accordance with Air Force Instruction (AFI) 33-332, Privacy Act Program, any data that are disseminated are required by DoD applications and organizations in the performance of official duties. All data transfers are via Secure LDAP and HTTPS using DoD Encryption methodologies in compliance with agreed upon Air Force and owning DoD organizations' Memorandums of Agreement (MOAs) and Interface requirements documents.

Individual Air Force members may view their personal data stored in the system by presenting their Common Access Card (CAC) and Personal Identifier Number (PIN). This two-factor authentication guarantees the individual has the proper credentials for the designated record. Data accessed by users are read only.

14. Describe whether the system derives or creates new data about individuals through aggregation.

The AFDS system generates an e-Mail for Life address for each active duty Air National Guard, Air Force Reservist, civilian and contractor in the Air Force. The e-Mail for Life address is in the format of first.last@us.af.mil. The e-Mail address is generated using the Electronic Digital Interchange Personal Identifier (EDIPI), name, and category code attributes that are stored within the system.

15. Describe with whom the information in identifiable form will be shared, both within the Component and outside the Component (e.g., other DoD Components, Federal agencies, etc.).

DoD personnel and applications will have access to all or some of the data elements contained in the AFDS meta-directory in accordance with their roles and responsibilities. AFDS engineers have complete access to the data in the system in order to resolve data conflicts and resolve technical complications. Access for data users is configured in compliance with negotiated Memorandums of Agreement (MOAs) between the application owner and AFDS. DoD applications will use the data contained in the AFDS meta-directory to satisfy various uses dependent on their design requirements. These applications are DoD projects and as such, are controlled by the appropriate directives and guidelines to ensure the proper protection is accorded to the data. Air Force members will only be able to access their individual record, and then only for verification purposes. In order for the member to retrieve their record they will have to present their Common Access Card (CAC) and Personal Identifier Number (PIN). This two-factor authentication guarantees the individual has the proper credentials for the designated record. Data accessed by users are read only.

16. Describe any opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses of the information in identifiable form. Where consent is to be obtained, describe the process regarding how the individual is to grant consent.

In compliance with AFI 33-332, Privacy Act Program, paragraph 12.4.1, any data released without consent of the subject are required in the performance of official duties.

All AFDS data are transferred via Secure LDAP and HTTPS using DoD encryption methodologies. All data collected are in compliance with agreed upon Air Force and owning organizations' Memorandums of Agreement (MOAs) and Interface requirements documents. Due to the nature of the data transfer, the information is not in identifiable form.

Air Force Privacy Act complaints process rules for accessing records, for contesting contents and for appealing initial agency determinations are published in AFI 33-332, Privacy Act Program, paragraph 1.3, Privacy Act Complaints; or they may be obtained from the system manager.

In accordance with AFI 33-332, Privacy Act Program, paragraph 12.4, Rules for Releasing Privacy Act Information without Consent of the Subject, individual consent is not required to disseminate the data stored in the AFDS System.

Exception 1 (DoD employees who have a need-to-know the information in the performance of their official duties) and Exemption 3 (The DoD 'Blanket Routine Uses' published at the beginning of the Air Force's compilation of System of Record Notices) apply to this system.

17. Describe any information that is provided to an individual, and the format of such information (Privacy Act Statement, Privacy Advisory) as well as the means of delivery (e.g., written, electronic, etc.), regarding the determination to collect the information in identifiable form.

AFDS customers are applications and organizations that have server-to-server links. All data transfers to AFDS customers are via Secure LDAP and HTTPS connections using approved DoD encryption methodologies. The only circumstance that AFDS would provide For Official Use Only (FOUO) data to an individual would be in allowing Air Force members to view the data contained in the system on themselves. Individual Air Force members will only be able to access their individual record for verification purposes. Individual service members are able to view the following information on themselves: EDIPI, Rank, First name, Middle name, Last name, Date of Birth, Citizenship Status, Duty Telephone Number - Commercial, Duty Telephone Number - DSN, e-Mail Address, Gender, Location, Major Command (MAJCOM), Assigned Unit, Social Security Number, Street Address, State, Zip Code, Service Code, Encryption PKI certificate Issues by DoD PKI, and Encryption PKI certificate published to Air Force GAL.

In order for the member to retrieve their record they will have to present their Common Access Card (CAC) and Personal Identifier Number (PIN). This two-factor authentication guarantees the individual has the proper credentials for the designated record. Data accessed by users is read only and is available through the AFDS Identity Management Portal (IMP).

18. Describe the administrative/business, physical, and technical processes and controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

The Privacy Impact Assessment (PIA) is based on proper implementation, validation, and verification of the baseline information assurance (IA) controls for CONFIDENTIALITY, in accordance with Department of Defense Instruction (DoDI) 8500.2, "Information Assurance Implementation." The controls address the administrative, physical, and technical controls required to secure, protect, and preserve the confidentiality of information in identifiable form.

AFDS is a mission assurance category (MAC) III system with a confidentiality level of "Sensitive." AFDS is currently certified and accredited and has implemented/validated the DoDI 8500.2 baseline controls for systems with a confidentiality level of "**SENSITIVE**."

The following controls apply to AFDS and systems with a confidentiality level of "SENSITIVE."

EBBD-2 Boundary Defense
EBPW-1 Public Wide Area Network Connection
EBRP-1 Remote Access for Privileged Functions
EBRU-1 Remote Access for User Functions
ECAD-1 Affiliation Display
ECAR-2 Audit Record Content – Sensitive Systems
ECAT-1 Audit Trail, Monitoring, Analysis, and Reporting
ECCR-1 Encryption for Confidentiality (Data at Rest)
ECCT-1 Encryption for Confidentiality (Data at Transmit)

ECIC-1 Interconnections among DoD Systems and Enclaves
ECLO-1 Logon
ECLP-1 Least Privilege
ECML-1 Marking and Labeling
ECMT-1 Conformance Monitoring and Testing
ECNK-1 Encryption for Need-to-Know
ECRC-1 Resource Control
ECRR-1 Audit Record Retention
ECTC-1 Tempest Controls
ECWM-1 Warning Message
IAAC-1 Account Control
IAGA-1 Group Identification and Authentication
IAIA-1 Individual Identification and Authentication
PRAS-1 Access to Information
PRMP-1 Maintenance Personnel
PRNK-1 Access to Need-to-Know Information
PRTN-1 Information Assurance Training
PECF-1 Access to Computing Facilities
PECS-1 Clearing and Sanitizing
PEDI-1 Data Interception
PEPF-1 Physical Protection of Facilities
PEPS-1 Physical Security Testing
PESP-1 Workplace Security Procedures
PESS-1 Storage
PEVC-1 Visitor Control to Computing Facilities
DCAS-1 Acquisition Standards
DCSR-2 Specified Robustness – Medium

System of Records Notice (SORN) Review: Records Access Procedures and Safeguards are adequately covered.

DoD personnel and applications will have access to all or some of the data elements contained in the AFDS meta-directory in accordance with their roles and responsibilities. AFDS engineers have complete access to the data in the system in order to resolve data conflicts and resolve technical complications. Access for data users is configured in compliance with negotiated Memorandums of Agreement (MOAs) between the application owner and AFDS. DoD applications will use the data contained in the AFDS meta-directory to satisfy various uses dependent on their design requirements. These applications are DoD projects and as such, are controlled by the appropriate directives and guidelines to ensure the proper protection is accorded to the data. Air Force members will only be able to access their individual record, and then only for verification purposes. In order for the member to retrieve their record they will have to present their Common Access Card (CAC) and Personal Identifier Number (PIN). This two-factor authentication guarantees the individual has the proper credentials for the designated record. Data accessed by users are read only. Authoritative sources can only change data that they are responsible for, all other data are read only.

19. Identify whether the IT system or collection of information will require a System of Records notice as defined by the Privacy Act of 1974 and as implemented by Department of Defense (DoD) Directive 5400.11, DoD Privacy Program, May 8, 2007; and DoD 5400.11-R, Department of Defense Privacy Program, May 14, 2007. If so, and a System Notice has been published in the Federal Register, the Privacy Act System of Records Identifier must be listed in question 6 above. If not yet published, state when publication of the Notice will occur.

A System of Records Notice (SORN) for AFDS, F033 AF E, was published in the Federal Register, February 25, 2005, 70 FR 9283.

20. Describe/evaluate any potential privacy risks regarding the collection, use, and sharing of the information in identifiable form. Describe/evaluate any privacy risks in providing individuals an opportunity to object/consent or in notifying individuals. Describe/evaluate further any risks posed by the adopted security measures.

Certification and Accreditation of the system revealed few security risks -- the Medium and Low risks were considered acceptable. Because access to all data requires authentication, it guarantees proper credentials for viewing/transferring any data. All data contained within AFDS are not in identifiable form. The data stored in the system are transferred via Secure LDAP and HTTPS using approved DoD encryption methodologies.

In accordance with AFI 33-332, Privacy Act Program, paragraph 12.4, Rules for Releasing Privacy Act Information without Consent of the Subject, individual consent is not required to disseminate the data stored in the AFDS System.

During the Certification and Accreditation process of AFDS, fourteen (14) residual risks were discovered. Of these, six (6) were rated as Medium and eight (8) were rated as Low. The Medium vulnerabilities are acceptable risks.

21. State classification of information/system and whether the Privacy Impact Assessment (PIA) should be published or not. If not, provide rationale. If a PIA is planned for publication, state whether it will be published in full or summary form.

Unclassified. This PIA will be published in full.

Privacy Impact Assessment Approval Page for Air Force Directory Services (AFDS)

[redacted] 24 July 07

Preparing Official
Name: [redacted]
Title: AFDS Program Manager
Organization: ~~HQ 754 ELSG/DONE~~
Work Phone Number: [redacted]
E-mail: [redacted]

[redacted] 26 Jul 07

Information Assurance Official
Name: [redacted]
Title: Commander
Organization: HQ AFCA/CC
Work Telephone Number: [redacted]
E-Mail: [redacted]

[redacted] 24 July 07

MAJCOM Privacy Act Official
Name: [redacted]
Title: Privacy Act Manager
Organization: HQ AFCA/CCQI
Work Telephone Number: [redacted]
E-mail: [redacted]

[redacted] 31 Jul 07

HQ Air Force Information Assurance Official
Name: [redacted]
Title: Information Assurance Officer
Organization: SAF/XCPPI
Work Telephone Number: [redacted]
E-mail: [redacted]

[redacted] 13 AUG 07

HQ Air Force Privacy Act Officer
Name: [redacted]
Title: Air Force Privacy Act Officer
Organization: SAF/XCPPA
Work Telephone Number: [redacted]
E-mail: [redacted]

[redacted] 14 Aug 2007

Reviewing Official
Name: [redacted]
Title: Air Force Chief Information Officer
Organization: SAF/XC
Work Telephone Number: [redacted]
E-mail: [redacted]